REMARKS

The Examiner rejected claims 1, 5-8, 10, 11 and 14 under 35 U. S. C. § 102. The Examiner relied on Albert U. S. Patent 5,991,410 (hereinafter Albert) to support this rejection. Claim 1 has been amended to incorporate limitations previously found in dependent claims. As a result, claim 10 has been cancelled without prejudice. Therefore, as to claim 10, this rejection is moot. As to claims 1, 5-8, 11 and 14, claim 1 has been amended to recite that the smartcard reader is a biometric smartcard reader able to obtain biometric data directly and that the smartcard contains biometric data. Claim 1 has also been amended to recite that the encrypted signal is transmitted from the biometric smartcard reader to a high security module at the remote location. Claim 1 has also been amended to recite

> "said signal [a signal created by said biometric smartcard reader dependent on a smartcard containing biometric data, said smartcard reader able to obtain biometric data directly] comprising access information dependent upon biometric data directly obtained by said biometric smartcard reader from a user and said biometric data contained in said smartcard."

Support for these amendments is found in the claims as originally filed, at page 6, lines 15-16 and 26-30, page 8, lines 13-14 and 19-31, page 10, line 10-page 11, line 6, page 16, lines 4-20, page 17, lines 1-2, page 18, lines 15-20, page 19, lines 1-10 of the specification as filed, in Figs. 7-10 as filed, and elsewhere in the application papers as filed.

Albert relates to the field of financial transaction processing and authorization, and more specifically to wireless data communications and data security for financial processing. Albert describes a wireless adapter for an existing financial transaction device compatible with the public switched telephone network (PSTN) to communicate wirelessly and a wireless financial transaction system. The existing financial transaction device is used with a wireless adapter and a wireless modem. A second wireless modem is connected to a host computer. Albert seeks to provide additional data security for the financial transaction between a host computer that communicates with an authorization processor and the financial transaction device. The wireless adapter receives financial information, indicative of financial transactions, in a PSTN compatible format, encrypts and converts the information into non-PSTN compatible format. The encrypted and converted information is transmitted to the host computer. The host computer decrypts the information and transmits the decrypted information to an authorization processor. The authorization processor transmits back to the host computer signals indicating authorization or denial of the financial transaction. The host computer transforms the signal received from the authorization

processor to the non-PSTN compatible format and transmits the authorization or denial signal to the existing financial transaction device.

Nor does Albert address the failure of conventional systems to protect against security breaches arising from a person getting into security lines in a wall to which a smartcard reader is connected. In such conventional security lines, false authorization signals and the like can be provided using known industry standards to signal an access controller in a remote location. The access controller provides or denies access to a location. Albert is entirely silent on this aspect. Consequently, there is nothing in Albert to suggest that such a smartcard reader mounted on a wall would not be defeated by sending false authorization signals to the access controller. Further, Albert does not disclose or suggest a high security module located remotely from the smartcard reader and at an inaccessible location relative to the smartcard reader.

Albert is also silent concerning a high security module at a remote location translating an encrypted signal to another format useable by the access controller. Albert does not disclose or suggest in any manner such combinations, and therefore cannot anticipate the invention as now claimed.

The Examiner rejected claims 2-4, 9, 16-24, 27 and 29-31 under 35 U. S. C. § 103. The Examiner relied upon the combination of Albert and Baratelli U. S. Patent 6,325,285 (hereinafter Baratelli) to support this rejection. Claims 2, 17 and 29-31 are cancelled without prejudice. Therefore, as to these claims, the rejection is moot. As to the remaining claims of this group, Baratelli describes a smartcard with an integrated fingerprint reader which comprises a CPU, a memory and a fingerprint reader including a sensing surface. The sensing surface is located along a surface of the smartcard to position an individual's thumb over the sensing surface when the card is inserted into a write/read unit. When an individual inserts the smartcard into the write/read unit, the smartcard creates an electrical representation of the individual's fingerprint and compares the acquired representation to a stored fingerprint representation in the smartcard's memory. If the created representation matches the stored representation, the smartcard is enabled, and the individual is given access to information and/or services that require cooperation of the smartcard. See the abstract of Baratelli. Baratelli thus teaches enabling of a smartcard and seeks to confirm the identity of an individual presenting a smartcard using biometrics, but does not require any of the individual's biometric information to be collected or stored by the write/read unit that is outside of the individual's control. See the summary of Baratelli.

Like Albert, Baratelli does not address conventional systems' failure to protect

against security breaches arising from a person getting into security lines in a wall to which a smartcard reader is connected. In such conventional security lines, false authorization signals and the like can be provided using known industry standards to signal an access controller in a remote location. The access controller provides or denies access to a location. Baratelli is entirely silent on this aspect. Consequently, there is nothing in Baratelli to suggest that such a smartcard reader mounted on a wall would not be defeated by sending false authorization signals to the access controller. Further Baratelli does not disclose or suggest a high security module located remotely from the smartcard reader and at an inaccessible location relative to the smartcard reader.

Baratelli is also entirely silent on a high security module at the remote location translating the encrypted signal to another format useable by the access controller. Baratelli does not disclose or suggest the claimed configuration, and thus, cannot anticipate or suggest the claimed configuration.

Since neither of Albert or Baratelli discloses or suggests these specifically recited elements of the claimed arrangement, no combination of them can fairly be said to disclose or suggest them. Applicant submits that the claims, as amended, are therefore patentable over any 35 U. S. C. § 103 obvious combination of Albert and Baratelli.

The Examiner rejected claim 12 under 35 U. S. C. § 103. The Examiner relied upon the combination of Albert and Delp U. S. Patent 6,922,558 (hereinafter Delp) to support this rejection. Claim 12 depends from claim 9, which depends from claim 1. The shortcomings of Albert are discussed above in connection with the discussion of the rejection of claim 1. Delp teaches nothing to overcome these deficiencies. Therefore, claim 12 is believed to be patentable over the combination of Albert and Delp.

The Examiner rejected claim 13 under 35 U. S. C. § 103. The Examiner relied upon the combination of Albert and Bartholomew U. S. Patent 5,724,417 (hereinafter Bartholomew) to support this rejection. Claim 13 depends from claim 9, which depends from claim 1. The shortcomings of Albert are discussed above in connection with the discussion of the rejection of claim 1. Bartholomew teaches nothing to overcome these deficiencies. Therefore, claim 13 is believed to be patentable over the combination of Albert and Bartholomew.

The Examiner rejected claim 15 under 35 U. S. C. § 103. The Examiner relied upon the combination of Albert and Renner U. S. Patent 6,223,984 (hereinafter Renner) to support this rejection. Claim 15 depends from claim 14, which depends from claim 1. The shortcomings of Albert are discussed above in connection with the discussion of the rejection

of claim 1. Renner teaches nothing to overcome these deficiencies. Therefore, claim 15 is believed to be patentable over the combination of Albert and Renner.

The Examiner rejected claim 25 under 35 U. S. C. § 103. The Examiner relied upon the combination of Albert, Baratelli and Delp to support this rejection. Claim 25 depends from claim 24, which depends from claim 16. The shortcomings of Albert and Baratelli are discussed above in connection with the discussion of the rejection of claim 16. Delp teaches nothing to overcome these deficiencies. Therefore, claim 25 is believed to be patentable over the combination of Albert, Baratelli and Delp.

The Examiner rejected claim 26 under 35 U. S. C. § 103. The Examiner relied upon the combination of Albert, Baratelli and Bartholomew to support this rejection. Claim 26 depends from claim 24, which depends from claim 16. The shortcomings of Albert and Baratelli are discussed above in connection with the discussion of the rejection of claim 16. Bartholomew teaches nothing to overcome these deficiencies. Therefore, claim 26 is believed to be patentable over the combination of Albert, Baratelli and Bartholomew.

The Examiner rejected claim 28 under 35 U. S. C. § 103. The Examiner relied upon the combination of Albert, Baratelli and Renner to support this rejection. Claim 28 depends from claim 27, which depends from claim 16. The shortcomings of Albert and Baratelli are discussed above in connection with the discussion of the rejection of claim 16. Renner teaches nothing to overcome these deficiencies. Therefore, claim 28 is believed to be patentable over the combination of Albert, Baratelli and Renner.

New claims 32 and 33 are submitted herewith. No new matter is sought to be entered by any of the amendments contained herein.

Applicant hereby petitions for a three month extension of the term for response to the July 16, 2007 official action to January 16, 2008. The Commissioner is hereby authorized to charge the $525.00 fee for this extension of time, as well as any other fees which are necessary to constitute this a timely response to the July 16, 2007 official action, to Applicant's undersigned counsel's deposit account 10-0435. A duplicate copy of this authorization is enclosed for this purpose.

Respectfully submitted,

Richard D. Conard
Atty. Reg. No. 27321
Attorney for Applicant

Indianapolis, Indiana
(317) 231-7285

INDS02 RDC 942868